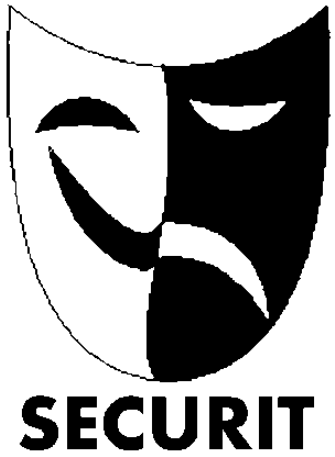


Security culture and information technology, SECURIT

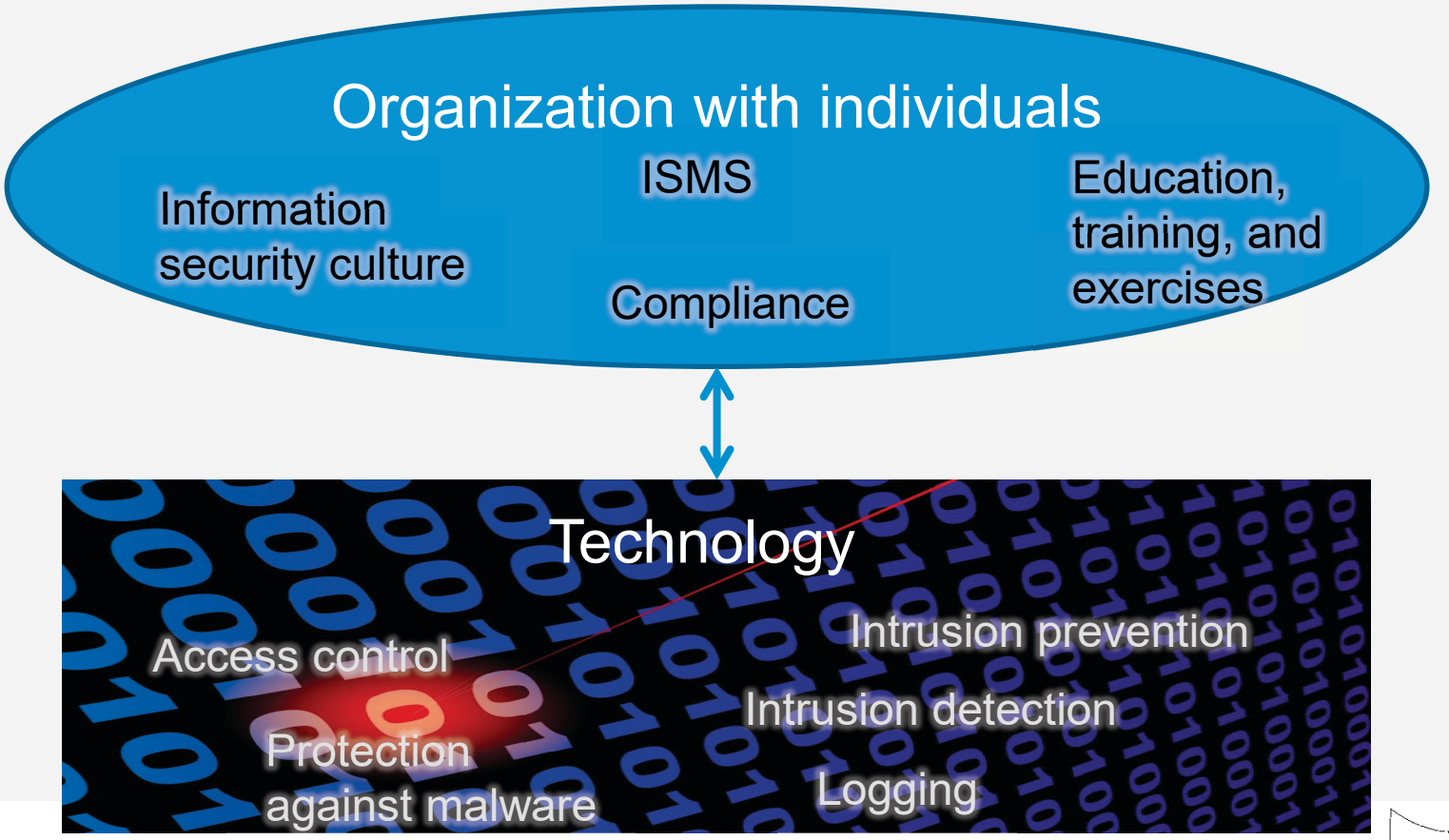
Jonas Hallberg

www.foi.se/securit

FOI

Information security

Information security includes social as well as technical aspects



www.foi.se/securit

SECURIT

What is culture?

Hofstede:

“Culture is the collective programming of the mind distinguishing the members of one group or category of people from others”

http://geert-hofstede.com/national-culture.html

Edgar Schein:

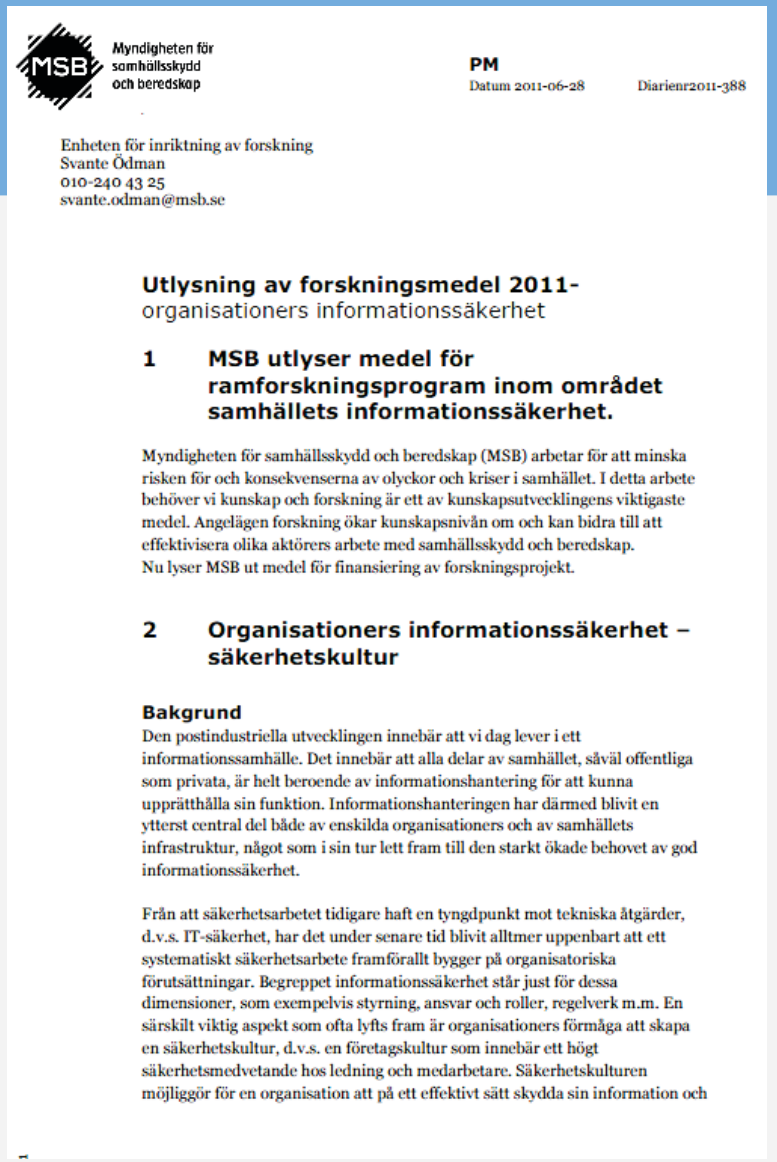
There are three distinct levels in

- Artifacts
- Espoused values
- Basic assumptions

Vital asset and risk source

Motivation

- The need for improved information security
- Security culture is vital for information security
- SECURIT studies
  - security-relevant characteristics of humans and organizations
  - the effects of applied social measures



Myndigheten för samhällsskydd och beredskap

PM
Datum 2011-06-28 Diarienr2011-388

Enheten för inriktning av forskning
Svante Ödman
010-240 43 25
svante.odman@msb.se

Utlysning av forskningsmedel 2011-
organisationers informationssäkerhet

1 MSB utlyser medel för ramforskningsprogram inom området samhällets informationssäkerhet.

Myndigheten för samhällsskydd och beredskap (MSB) arbetar för att minska risken för och konsekvenserna av olyckor och kriser i samhället. I detta arbete behöver vi kunskap och forskning är ett av kunskapsutvecklingens viktigaste medel. Angelägen forskning ökar kunskapsnivån om och kan bidra till att effektivisera olika aktörers arbete med samhällsskydd och beredskap.
Nu lyser MSB ut medel för finansiering av forskningsprojekt.

2 Organisationers informationssäkerhet – säkerhetskultur

Bakgrund
Den postindustriella utvecklingen innebär att vi dag lever i ett informationssamhälle. Det innebär att alla delar av samhället, såväl offentliga som privata, är helt beroende av informationshantering för att kunna upprätthålla sin funktion. Informationshanteringen har därmed blivit en ytterst central del både av enskilda organisationers och av samhällets infrastruktur, något som i sin tur lett fram till den starkt ökade behovet av god informationssäkerhet.

Från att säkerhetsarbetet tidigare haft en tyngdpunkt mot tekniska åtgärder, d.v.s. IT-säkerhet, har det under senare tid blivit alltmer uppenbart att ett systematiskt säkerhetsarbete framförallt bygger på organisatoriska förutsättningar. Begreppet informationssäkerhet står just för dessa dimensioner, som exempelvis styrning, ansvar och roller, regelverk m.m. En särskilt viktig aspekt som ofta lyfts fram är organisationers förmåga att skapa en säkerhetskultur, d.v.s. en företagskultur som innebär ett högt säkerhetsmedvetande hos ledning och medarbetare. Säkerhetskulturen möjliggör för en organisation att på ett effektivt sätt skydda sin information och

www.foi.se/securit

SECURIT

The SECURIT research consortium

MSB Myndigheten för samhällsskydd och beredskap

KTH VETENSKAP OCH KONST

LINKÖPINGS UNIVERSITET

GÖTEBORGS UNIVERSITET

ÖREBRO UNIVERSITET

CHALMERS

FOI

KARLSTADS UNIVERSITET

www.foi.se/securit

SECURIT

The SECURIT program, 2012-2017

Information security culture:
Shared patterns of thought, behaviour, and values that arise and evolve within a social group, based on communicative processes influenced by internal and external requirements, are conveyed to new members and have implications on information security.

http://foi.se/sv/Sok/Sammanfattningssida/?rNo=FOI+MEMO+5253

www.foi.se/securit

SECURIT

The research projects in SECURIT

Research projects

The main research efforts carried out within the SECURIT are performed in the nine research projects included in the program.

In the below figure, the scheduling of the projects is illustrated. Overviews of the projects are provided in the following subsections. The results are continuously disseminated through scientific publication and other forms of presentation.

www.foi.se/securit

SECURIT

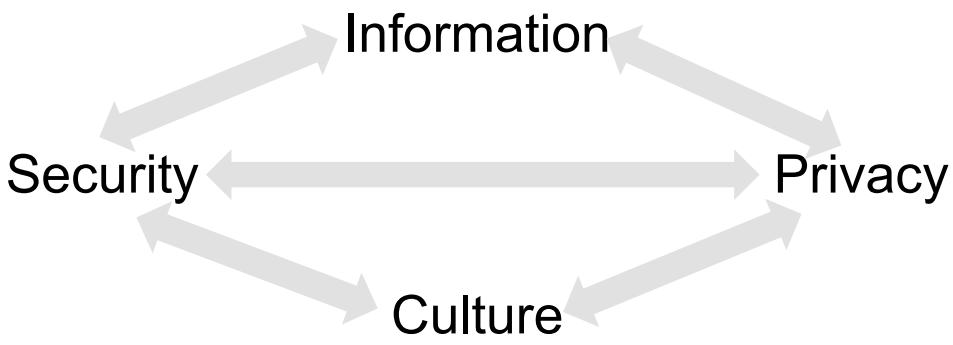
SECURIT project managers

- Security culture: **Sven Ove Hansson**, KTH
- User acceptance of information security policies: **Jonas Hallberg**, FOI
- Attitude, culture, and information security: **Anders Pousette**, Göteborgs universitet
- Discourse and security practice: **Peter Johansson**, Göteborgs universitet
- Balanced IT-based Organizational development: **Jonas Landgren**, Göteborgs universitet/Chalmers
- ATTITUDE: **Joachim Åström**, Örebro universitet
- INTERORG: **Frans Prenkert**, Örebro universitet
- CONGRUENCE: **Fredrik Karlsson**, Örebro universitet
- Cultural aspects in information security standard development, **Fredrik Karlsson**, Örebro universitet

Statistics Sweden (SCB) survey

- Items assembled from several projects
- Distribution
  - 11 000 employees
  - 120 organizations
  - 6 industries

Philosophical Perspectives on: Information Security Culture



Examples of Research Question:

- What is (semantic) information?
- When is some information (system) secure?
- How do we define privacy and the right to privacy?
- Are there thematic sub-cultures, such as a security or privacy culture?
- How should we understand security tradeoffs, in particular failed tradeoffs?

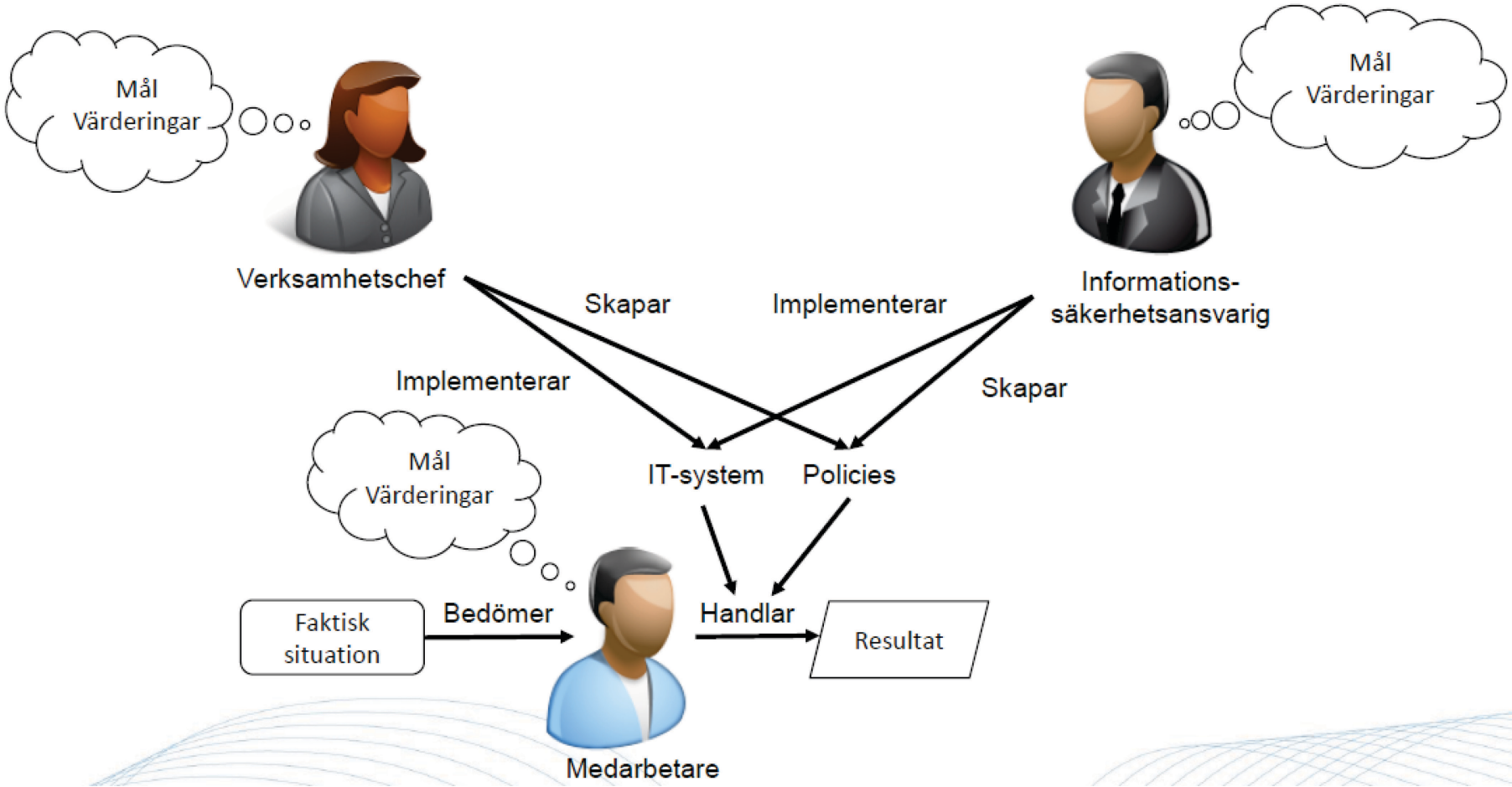
Project Participants: Sven Ove Hansson, Niklas Möller, Björn Lundgren
Division of Philosophy, KTH – Royal Institute of Technology, Brinellvägen 32, SE-100 44 Stockholm
Contact: bjorn.lundgren@abe.kth.se +46(0)8 – 790 9425

Attitude

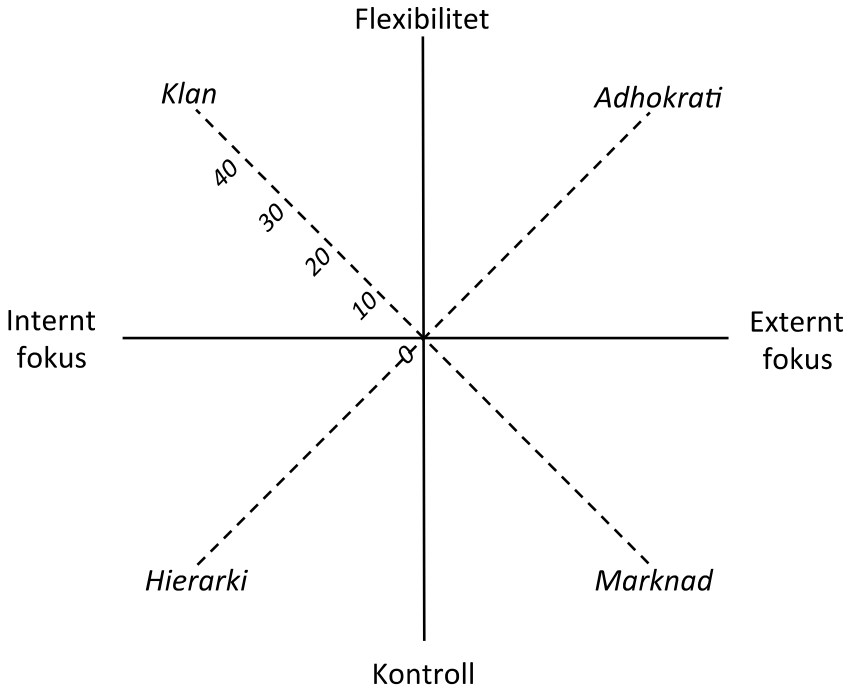
The aim of the project is to foster a greater understanding of how organisational cultures mediate and effect different actors information security behaviour.

Publications, e.g.: Karlsson F, Åström J, Karlsson M (2015) Information security culture : State-of-the-art review between 2000 and 2013. Information Management & Computer Security, Volume 23, Issue 3, 246-285.

Flera samtida värdesystem



Competing Values Framework



Operationaliseringen av de fyra kulturtyperna tycks fungera bra, enligt en faktoranalys.

Lite skakigare när det gäller adhocracy och market än övriga pga liten representation där.

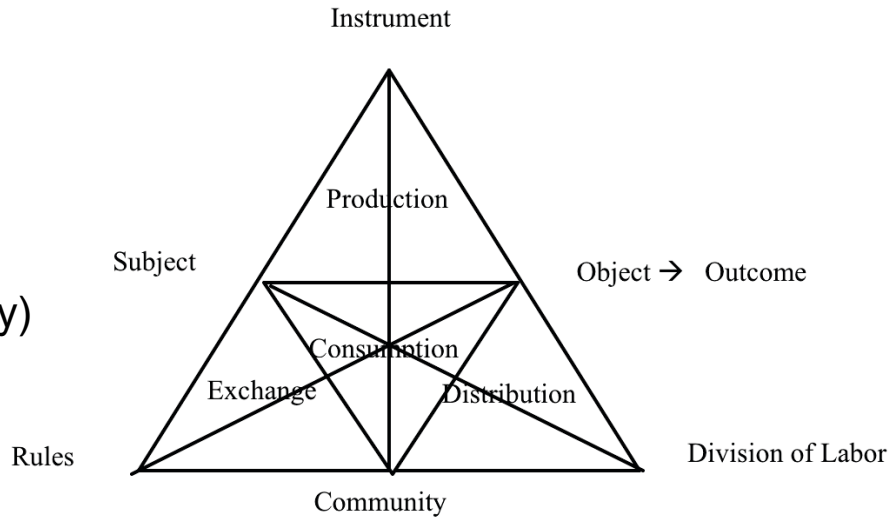
Interorg 1(2)

The aim of the INTERORG project is to develop knowledge of the character of conflicts between information security cultures in inter-organizational contexts.

Case: the Swedish Nuclear Fuel and Waste Management Company (SKB) and the Swedish NGO Office for Nuclear Waste Review (MKG)

Analytical frameworks:

- CHAT (Cultural-Historical Activity Theory)
- ANT (Actor-Netwok Theory)
- CIA & RITE-principles



Interorg 2(2)

Analysis of how CIA & RITE-principles evolve in an inter-organisational setting. This analaysis is based on ANT.

Information sharing is analysed using CHAT.

Publications, e.g.: Karlsson F, Kolkowska K, Hedström K, Frostenson M (2015) Inter-organisational information sharing – between a rock and a hard place. 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), Lesvos, Greece, July 1-3 July, 2015.

Karlsson F, Kolkowska K, Prenkert F (Accepted) Inter-organisational information security: a systematic literature review. Information and Computer Security

Congruence 1(2)

The aim of the CONGRUENCE project is to develop knowledge on how to ensure that the tools used to transform the information security culture in an organization are in harmony, clearly and with certainty communicating the organization's information security culture.

The final deliverables will support: 1) identification of challenges, and 2) guidelines for how to manage congruent information security and related artifacts.

Developed 8 tentative quality criteria for information security policies

Publications, e.g.: Karlsson F, Goldkuhl G, Hedström K (2015) Information Security Policy in Health Care – from Practice-Based Discourse Analysis to Tentative Quality Criteria. the 30th International Information Security and Privacy Conference, Hamburg, Germany, May 26-28, 2015.

Congruence 2(2)

The developed quality criteria will be used in the forthcoming analysis of a larger set of information security policies. Aim:

- To validate the criteria
- To identified problematic aspects in achieving congruent communication using information security policies.

Cases studies will be carried out to investigate communication aspects further, and their impact on culture.

Cultural aspects on information security standard development 1(3)

- Standards are everywhere
- Can be seen as a system of ‘global order’
- Are supposed to be based on “best practices”

Cultural aspects on information security standard development 2(3)

The project will uncover the co-construction of information security standards and culture behind information security standard making.

- Interpretive ethnography research method
- Project/data collection at Swedish Standards Institute/TC 318
- Longitudinal study

Analysis Part I

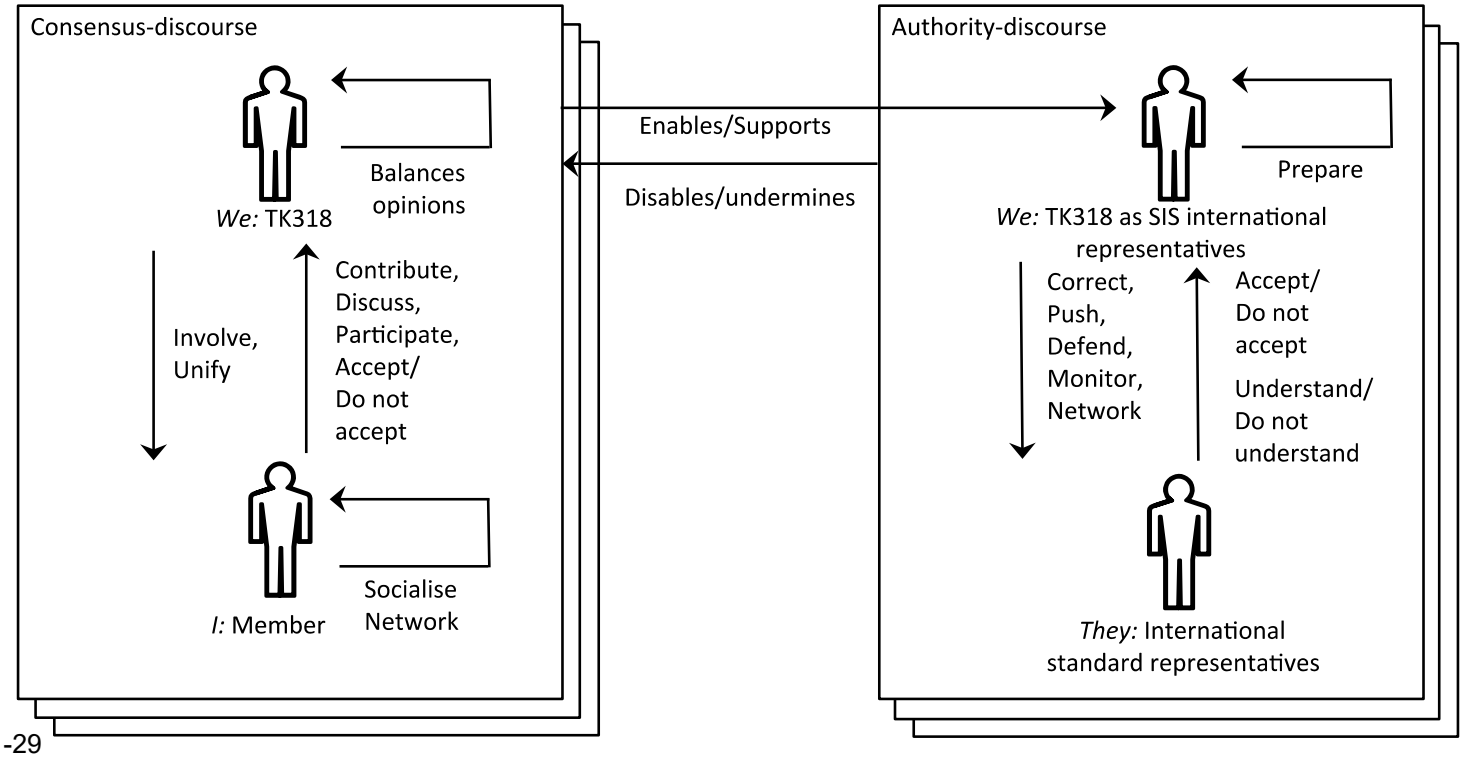
Analysis using discourse (completed)

Analysis Part II

Analysis using Structuration theory

Cultural aspects on information security standard development 3(3)

Result of part I: Model of two conflicting discourses at play in information security standards-making



GÖTEBORG UNIVERSITY

Attitude, culture and information security
Pousette, Törner & Skyvell-Nilsson

Study 1

- Aim: To describe the process of formation of a security culture in healthcare, and the rational grounds among healthcare practitioners that may explain the quality of the emerging culture.
- Research question: How does information security culture emerge in the tension between the rationalities emanating from the design of the information technology, information security policies, organizational production demands, professional cultures and patients' needs?
- Method: Step 1: Interviews with leaders and IS professionals to develop scenarios. Step 2: Interviews with health care personnel based on scenarios.
- Time: 2013-2015

GÖTEBORG UNIVERSITY

Attitude, culture and information security
Pousette, Törner & Skyvell-Nilsson

Study 2

- Aim: To investigate the influence of information security climate on information safety practice in day-to-day work
- Research question: What is the influence of different aspects of the IS climate on safety behavior (compliance and participative)
- Method: Quantitative multilevel study (individuals in workplaces in organizations) based on questionnaires to operative personnel and managers within selected industries.
- Time: 2014-2017

Discourse and Security Practice

- Information Security (IS) is part of a wider context where discourses focusing on human rights and democratic values are articulated to both support and counteract IS initiatives.
- IS systems can be used to further human rights such as personal security and privacy (e.g. regulating access to medical journals), but IS implementation can also threaten and abuse core values in a democratic society.
- The challenge is not only to create IS systems that protect information on a technological level and ensure compliance among its users (the user-as-risk factor), but to create systems and policies that take other values and interests into account, such as accountability, transparency, freedoms of expression and information, and privacy.
- Fundamental and critical questions are; Who is responsible to safe-guard that human rights and democratic values are taken into consideration when IS systems (including both technology and policies) are developed? To what extent are such considerations made when IS systems are developed?

Discourse and Security Practice
Aims and Goals

- Aims

– to investigate how discourses on human rights and democratic values inform and influence the development of information security systems where large quantities of sensitive data on citizens and patients are collected and stored.

– to investigate attitudes to whistleblowing and freedom of information and how these values affect behaviour and attitudes relating to information security systems

Discourse and Security Practice
Aims and Goals

- Goals relating to the first aim

– to inform how concepts and norms linked to the human rights discourse (such as individual privacy) are interacting and competing with public and private interests in the development of information systems collecting and storing large quantities of sensitive data on citizens and patients

– to problematize assumptions about the individual/patient as a rational, autonomous and socially independent actor who can make appropriate decision in a context characterised by uncertainties about the cumulative effects on privacy and information security

- Conclusions

– Clear trend towards an increase in privacy self-management that puts an increased responsibility on the individual to handle privacy issues and information security

– Privacy concerns is often seen as conflicting with what is considered the ultimate priority in health care services — saving lives.

– There is a lack of a thorough discussions concerning privacy in the development and implementation stages of new technological platforms in the health care sector in Sweden.

Discourse and Security Practice
Aims and Goals

- Goals relating to the second aim

– to measure attitudes towards whistleblowing and freedom of information
– to analyse the link between attitudes towards whistleblowing and freedom of information and attitudes towards information security regulations
– to analyse the link between attitudes towards whistleblowing and freedom of information and information security behaviour

- Conclusions

– To be revealed after survey data analysis during the autumn of 2016. ☺

Balanced IT-based organizational development 1(2)

- Challenge: provide a viable balance between security, usability, personal integrity, and human rights
- Aim: investigate how IT-based organizational development could be shaped to improve design, implementation and use of information systems
- Research setting: the network of actors involved in emergency response, including SOS-Alarm, local fire brigade, and regional paramedics
- Paper: the challenges of making use of social media for operators in emergency response work
  - difficult to adopt and embed in the existing work culture and information management practice

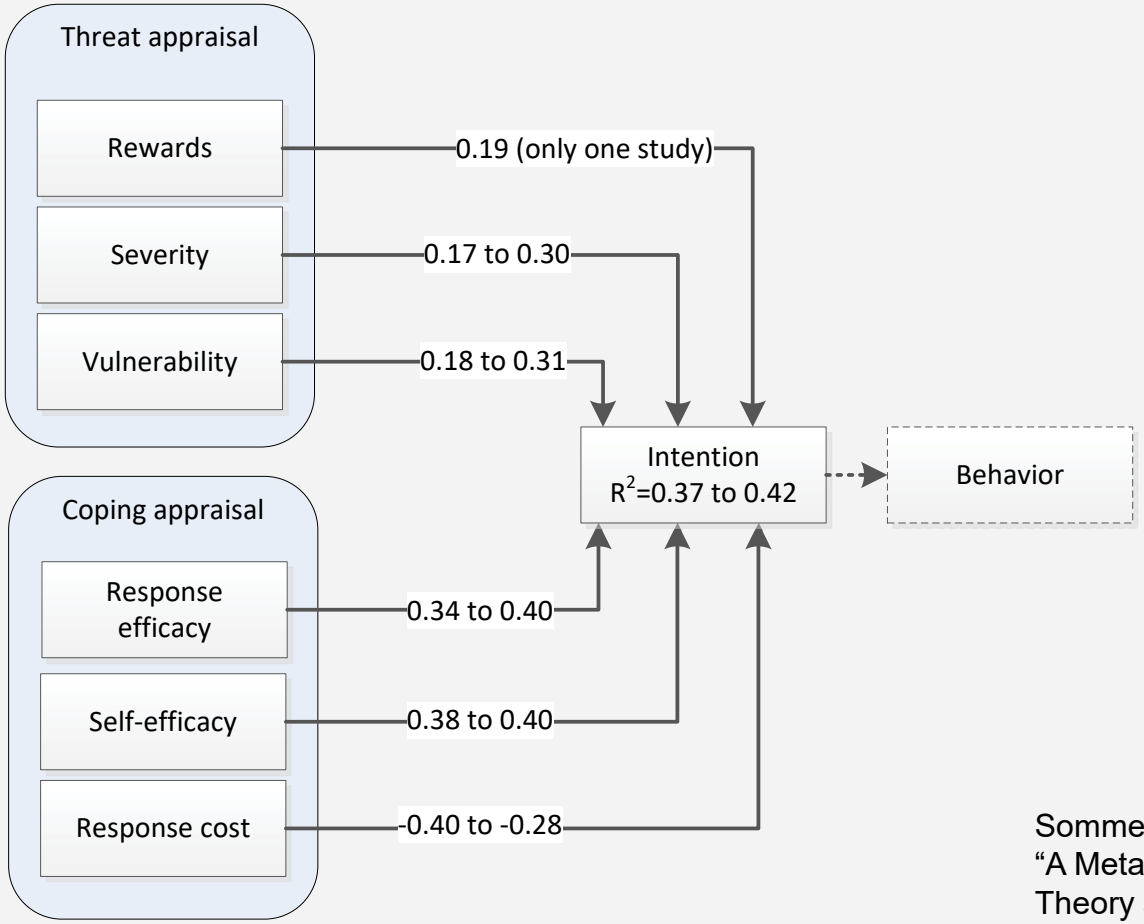
Balanced IT-based organizational development 1(2)

- Conclusions
  - There is an clear risk that demands on increased security in reality will result in decreased security
  - Achieving information security could be developed into a collaborative effort between the core business and the supporting activities of domain experts

User acceptance of information security policies

- **Theme 1**: Factors influencing the compliance with information security policies and similar security-related behavior within organizations
- **Theme 2**: The risk perceptions of individuals and groups and the relationship between information security risk perceptions, policies, and compliance
- **Theme 3**: Information security incident models and the effect on the information security of organizations

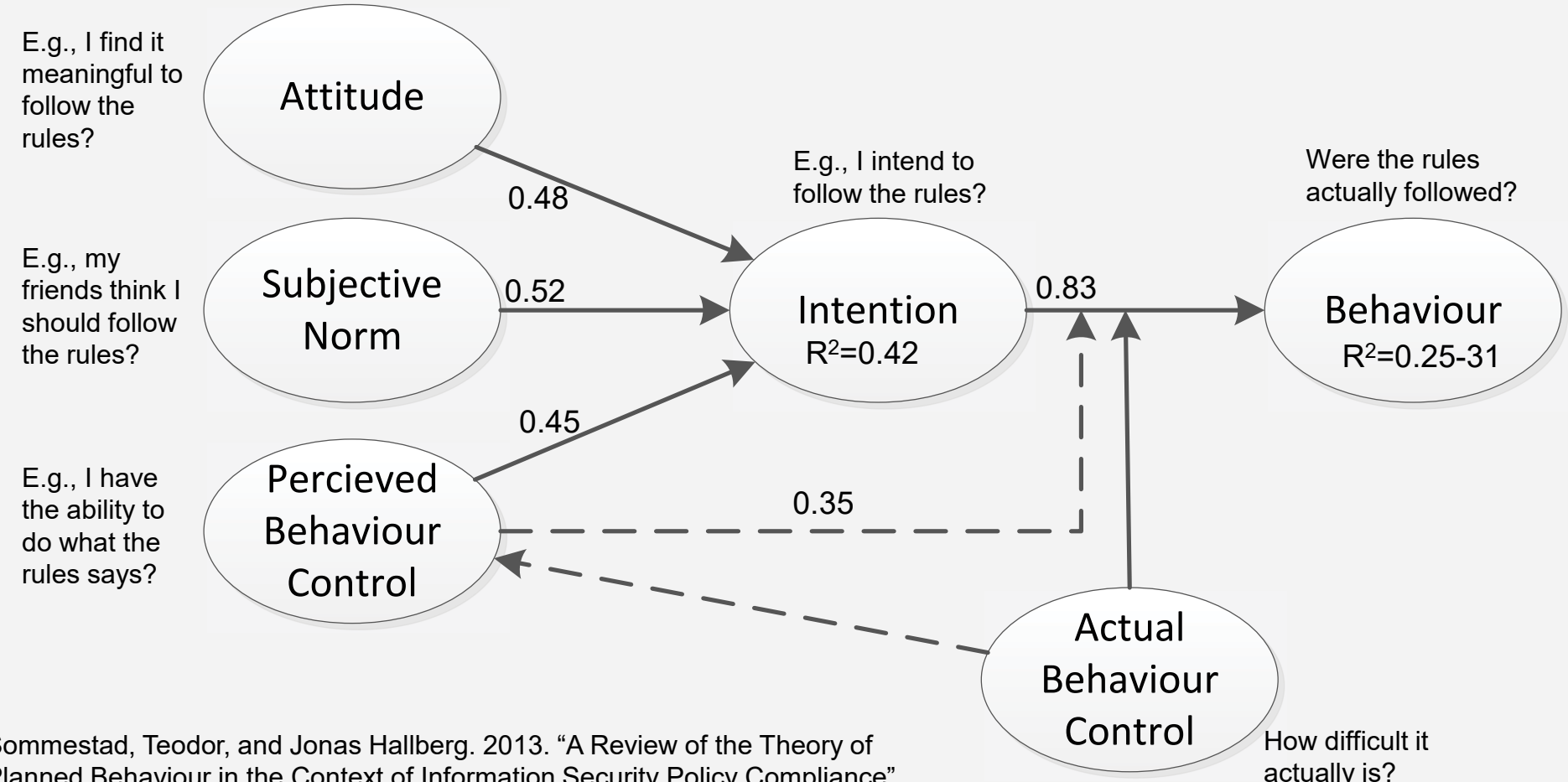
User acceptance of information security policies
Theme 1: Protection Motivation Theory



- It matters if it is:
  - Compliance or secure behavior
  - Threats to you or threats to others
  - Generic or specific behavior

Sommestad, Teodor, Henrik Karlzén and Jonas Hallberg, "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behavior"

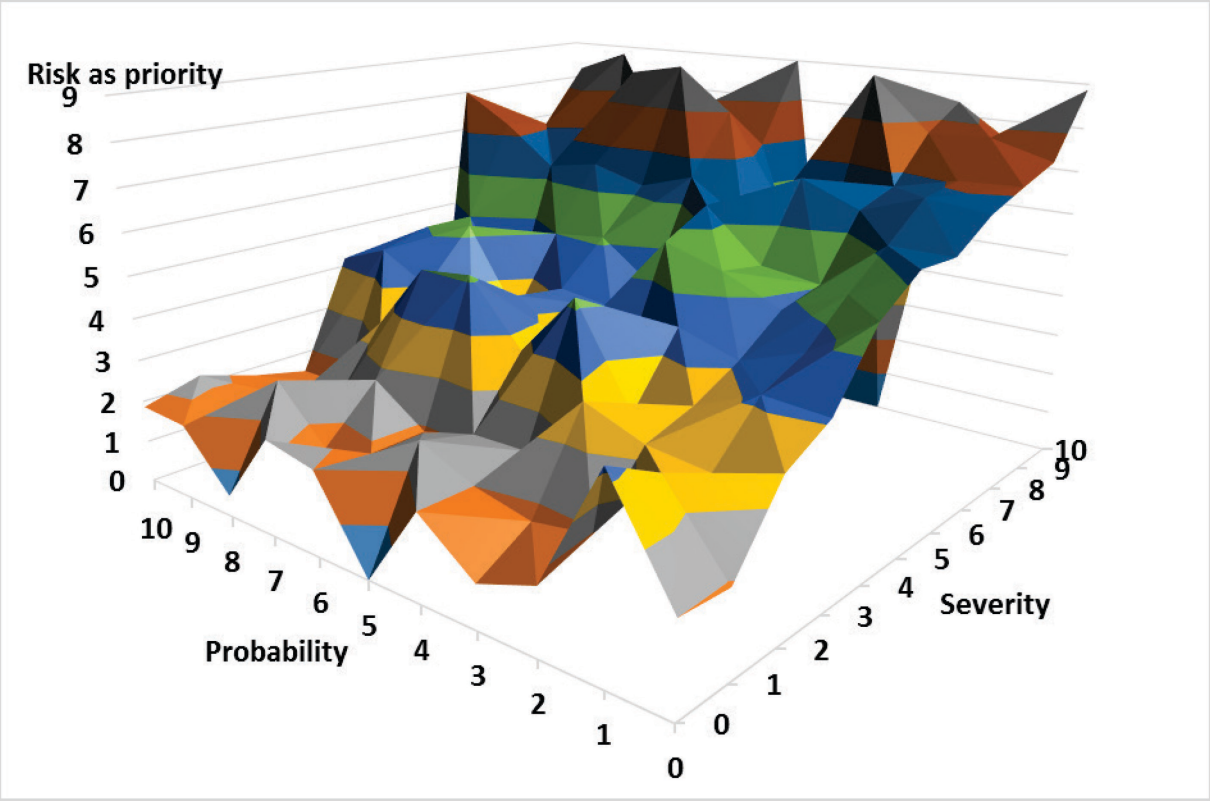
User acceptance of information security policies
Theme 1: Protection Motivation Theory



Sommestad, Teodor, and Jonas Hallberg. 2013. "A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance"

SECURIT

User acceptance of information security policies
Theme 2: How do people do their information security risk calculations?



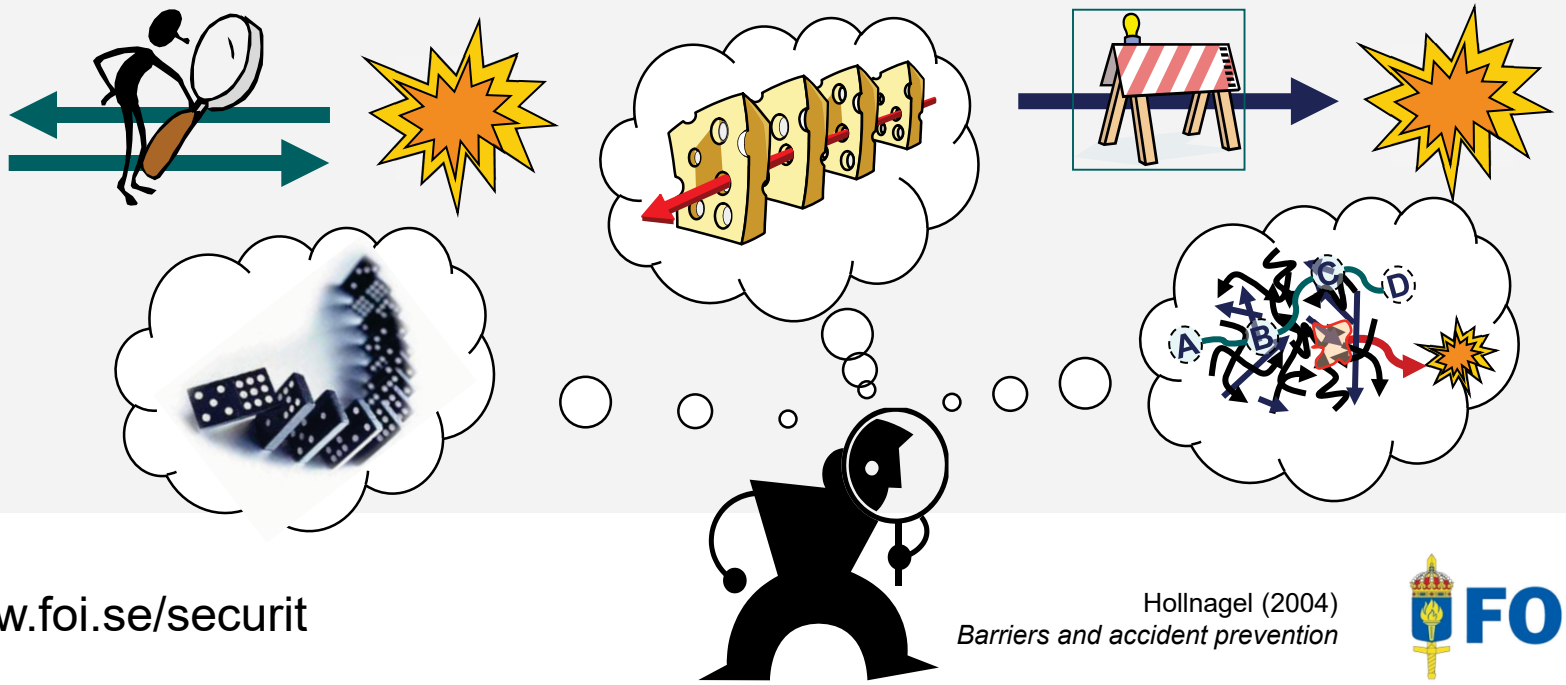
T. Sommestad, H. Karlzén, P. Nilsson, J. Hallberg, (2016) "An empirical test of the perceived relationship between risk and the constituents severity and probability", Information & Computer Security, Vol. 24 Iss: 2

www.foi.se/securit

SECURIT

User acceptance of information security policies
Theme 3: Information security incident models and management

- Questionnaires/interviews within a few strategically selected organizations/roles concerning “information security incident models”.



Hollnagel (2004)
Barriers and accident prevention

FOI